Vedlegg 6

20.10.2020

Versjon: 0.9

# Databehandleravtale UTKAST

## Minibuss- og personbiltjenester Follo 2022

# Databehandleravtale

Basert på Vedlegg 3 til Bransjenorm for Behandling av Personopplysninger i elektronisk billettering (Bransjenormen).

Oppdatert av Ruter etter krav i ny personopplysningslov og EU forordning 2016/679 - GDPR

Mellom

Ruter AS
Behandlingsansvarlig

Og

[Navn på Operatør]
Databehandler

# Innhold

# 1. Avtalens formål

Avtalens formål er å regulere rettigheter og plikter etter gjeldende personopplysningslov og personvernforordning (GDPR). Avtalen skal sikre at Personopplysninger om den registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer Databehandlers bruk av Personopplysninger på vegne av den Behandlingsansvarlige – herunder innsamling, registrering, sammenstilling, lagring, videreformidling, utlevering eller kombinasjoner av disse.

Meddelelser etter denne avtalen skal sendes skriftlig til personvernombud@ruter.no**.**

# 2. Definisjoner

Det vises til definisjonene i Kontrakt Busstjenester Oslo sør 2021, også kalt Hovedavtalen. I tillegg gjelder følgende definisjoner:

**Behandlingsansvarlig:** Den som bestemmer formålet med behandlingen av Personopplysninger og hvilke hjelpemidler som skal brukes. Ruter er behandlingsansvarlig i denne avtalen.

**Databehandler:** Den som behandler Personopplysninger på vegne av den Behandlingsansvarlige. Operatøren er behandlingsansvarlig i denne avtalen.

**Personopplysninger:** Opplysninger og vurderinger som kan knyttes til en enkeltperson.

**Behandling av personopplysninger:** Enhver bruk av Personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

**Behandlingsformål**:
Angir hensikten med behandlingen av Personopplysninger. Databehandler skal utføre konkrete oppgaver (driftsformål) for å oppfylle behandlingsformålet.

**Rettslig grunnlag (behandlingsgrunnlag):**
Grunnlag som gjør behandlingen av Personopplysninger lovlig. Samtykke fra den registrerte er et praktisk behandlingsgrunnlag.

# 3. Behandlingsformål og Rettslig grunnlag

Databehandler skal kun behandle Personopplysninger som er i samsvar med formålet og for øvrig i samsvar med Hovedavtalen.

**Formålet med behandlingen er:**
Oppfølging av klagesaker fra kunden om den utførte transport som Operatør får oversendt av Oppdragsgiver.

Operatøren får tilgang til kjøretøydata i sanntid som kan knyttes til sjåførene. Slik data kan bare behandles videre av Operatøren, for eksempel i forbindelse med oppfølging av sjåførene, dersom dette skjer innenfor rammen av gjeldende lovverk. Operatøren har ansvaret for at spørsmålet på forhånd blir drøftet med tillitsvalgte. Operatøren vil være Behandlingsansvarlig for behandling av kjøretøydata i sanntid til et slikt formål.

**Rettslig grunnlag for behandlingen:**
Behandlingsansvarlige bekrefter at Behandlingsansvarlig har tilstrekkelig hjemmelsgrunnlag for Behandling av Personopplysninger, og har rett til, og ansvaret for lovligheten av, overføring av personopplysningene til Databehandler.

Aktuelt grunnlag er kundens samtykke, eller at behandlingen er nødvendig for å oppfylle en transportavtale med kunden.

**Personopplysningskategorier:**
Databehandler vil kunne få tilgang og behandle følgende personopplysnings-kategorier:

- Navn, adresse, fødselsdato, e-postadresse, telefonnummer og lignende kontaktopplysninger, og angivelse av klageårsak.
- Det behandles også opplysninger om sjåfør ID, reell avgangstid og opplysninger knyttet til oppgjør av sjåførens kasse så som salgsbeløp og saldo. For tiden behandles også sjåførnavn, men det planlegges strøket.

**Tidsavgrenset behandling:**
Sletting av personopplysningene skal skje i samsvar med Behandlingsansvarliges sletterutiner, eller etter Behandlingsansvarliges instruks ,og i samsvar med gjeldende lovverk.

Databehandler skal kunne behandle Personopplysninger i den grad det er nødvendig for å oppnå ovennevnte formål. Opplysningene kan uansett ikke lagres lengre enn et år etter at de ble mottatt.

Personopplysningene kan ikke benyttes for Databehandlers formål, med mindre det følger av denne avtale.

# 4. Den Behandlingsansvarliges rolle

Behandlingsansvarlig bestemmer over behandlingen av Personopplysninger som omfattes av denne avtale.

Ruter er som Behandlingsansvarlig bl.a. ansvarlig for at det foreligger et lovlig behandlingsgrunnlag for personopplysningene, og at den aktuelle behandling er i overensstemmelse med gjeldende lovgivning.

Med mindre annet følger av lov, har den Behandlingsansvarlige rett til tilgang til og innsyn i både personopplysningene som behandles, og i systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

# 5. Databehandlerens plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som den Behandlingsansvarlige til enhver tid har bestemt skal gjelde.

Dersom ikke annet er avtalt skal personopplysningene ikke benyttes til andre formål enn det som er beskrevet i denne avtalen.

Databehandler er ansvarlig for å oppfylle følgende pliktene i EU forordning 2016/679 for Behandling av Personopplysninger (men ikke avgrenset til):

- Varsle Behandlingsansvarlig om avvik uten unødvendig forsinkelse, slik at Behandlingsansvarlig kan oppfylle fristen til å varsle Datatilsynet innen 72 timer jf.artikkel 33.
- Opprette personvernombud dersom man behandler Personopplysninger i stor målestokk, eller dersom man behandler sensitive Personopplysninger i stort omfang eller er offentlig virksomhet. jf. art 37 og 38.
- Yte nødvendig bistand til Behandlingsansvarlig i oppfyllelsen av den registrertes rettigheter slik de er beskrevet i GDPR kapitel 3, herunder retten til å kreve sletting, retting og innsyn i personopplysningene, retten til å kreve begrensning av en behandling og dataportabilitet mm.
- Underrette den Behandlingsansvarlige dersom de mener at instruksjonene de mottar er i strid med forordningen eller andre personvernregler.
- Ivareta forsvarlig informasjonssikkerhet ved egen behandling, jf. GDPR art 32, se under punkt 9.

I tillegg skal Databehandler bistå Behandlingsansvarlig i utarbeidelsen av DPIA etter GDPR art 35.

Brudd på pliktene kan føre til sanksjoner fra Datatilsynet, jf. GDPR artikkel 58 og fortalen nr.146.

Dersom Behandlingsansvarlig blir erstatningsansvarlig overfor den registrerte, eller blir ilagt bøter, er Databehandler ansvarlig for tap som er forårsaket av at han ikke har oppfylt forpliktelser i denne forordningen, eller hvis han har handlet i strid med Behandlingsansvarliges instruks for behandlingen

# 6. Taushetsplikt

Databehandler har taushetsplikt om dokumentasjon og Personopplysninger som vedkommende får tilgang til iht. denne avtalen. Dette gjelder også etter avtalens eller ansettelsesforholdets eller tjenesteforholdets opphør.

# 7. Bruk av skytjenester – overføring av opplysninger til land utenfor EUØ/EØS

Databehandler eller hans underleverandører, kan ikke benytte «sky tjenester» dersom dette kan medføre at Personopplysninger behandles utenfor EU/EØS, uten at dette er særskilt godkjent av Behandlingsansvarlig. Dette inkluderer lagring av Personopplysninger på server utenfor EU/EØS og at noen av leverandørens eller underleverandørens ansatte kan få tilgang til system hvor det behandles Personopplysninger. Tilsvarende gjelder for innlogging via skytjenester.

Dersom Behandlingsansvarlig gir slik godkjenning skal Databehandler sikre og dokumentere at det finnes gyldig Rettslig grunnlag for Behandling av Personopplysninger utenfor EU/EØS. Databehandler skal på forhånd sørge for nødvendig risikovurdering, som skal forelegges Behandlingsansvarlig til godkjennelse.

Sensitive Personopplysninger kan uansett ikke behandles utenfor EU/EØS uten kryptering. Spørsmål om behandling av Personopplysninger i forbindelse med skytjenester skal uansett tas opp med Behandlingsansvarlig senest tre måneder før oppstart av Behandling av personopplysninger.

# 8. Bruk av underleverandør

Behandlingsansvarlig skal godkjenne Databehandlers eventuelle bruk av underleverandører før behandlingen av Personopplysninger starter. Underleverandører som er godkjent ved oppstart av avtalen skal vedlegges hovedavtalen.

Underleverandøren skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser, og oppfylle disse på lik linje med Databehandler.

En oversikt over underleverandører som ved avtaleinngåelsen - eller på et senere tidspunkt - skal behandle Personopplysninger vedlegges databehandleravtalen, jf bilag 1 Oversikt over godkjente underleverandører.

Databehandler er ansvarlig overfor Behandlingsansvarlig for avtalebrudd som eventuelle underleverandører til tjenesten gjør seg skyldig i. Dersom en underleverandør ikke lengre har gyldig Rettslig grunnlag til å behandle Personopplysninger skal Databehandler sørge for at tjenesten fortsatt kan tilbys ved at man skaffer en ny underleverandør, eller alternativt utfører tjenesten selv.

# 9. Informasjonssikkerhet

Databehandler skal sørge for forsvarlig informasjonssikkerhet i sine systemer for Behandling av Personopplysninger og annen informasjon knyttet til oppdraget for Ruter. Behandlingsansvarlig kan kreve å få fremlagt gjennomførte risikovurderinger.

Databehandler skal etablere og holde en oversikt over sikkerhetstiltak som risikovurderinger har avdekket behov for.

Databehandler skal ha en dokumentert autorisasjonsordninger for ansatte som skal få tilgang til å behandle Personopplysninger. Databehandler må sørge for å ha forsvarlig sikring av servere, databaser og annet tilsvarende utstyr slik at ingen uvedkommende kan få tilgang til Personopplysninger. Det samme gjelder utskrifter og utfylte skjemaer.
For å oppfylle disse kravene, har Databehandler plikt til å dokumentere sine sikkerhetsrutiner. Dokumentasjonen skal gjøres tilgjengelig for Behandlingsansvarlig.

Databehandler skal ha et styringssystem. Systemet skal omfatte, men skal ikke avgrenses til, rutiner for:

- Avviksbehandling som omfatter varsling ved feil bruk av informasjonssystemet, herunder sikkerhetsbrudd.
- Sikkerhetsrevisjon, herunder jevnlig oversendelse av rapporter fra sikkerhetsrevisjoner.
- Ledelsens gjennomgang av sikkerhetsarbeidet.
- Gjennomføring av årlige revisjoner av virksomheten.

Avviksmelding skal skje ved at Databehandler uten unødvendig opphold melder avviket til Behandlingsansvarlig. Den Behandlingsansvarlige har ansvaret for at avviksmelding sendes Datatilsynet, dersom dette er påkrevet.

Databehandler skal bistå Behandlingsansvarlig slik at han kan ivareta sitt eget ansvar etter lov og forskrift bla ved:

- Varsling av avvik, jf. punkt 5
- Bistå Behandlingsansvarlig med blant tekniske data og fakta om tjenesten ved utarbeidelse av nødvendig konsekvensanalyse og risikovurdering.
- Informasjonsutveksling med Behandlingsansvarlig om nye lover og regler, praksis og annet som kan ha betydning for å oppfylle krav til god informasjonssikkerhet.

Databehandler skal oppfylle øvrige krav til sikkerhetstiltak som stilles etter gjeldende personopplysningslov og GDPR art 32 og 33.

# 10. Sikkerhetsrevisjoner

Behandlingsansvarlige skal kunne gjennomføre sikkerhetsrevisjoner av Databehandler. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Databehandler plikter å bistå Behandlingsansvarlig med slike revisjoner og gjøre nødvendig dokumentasjon tilgjengelig.

# 11. Avtalens varighet og endringer

Avtalen gjelder så lenge Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig. Dette tidspunktet vil i praksis være knyttet til Hovedavtalens utløp.

Ved brudd på avtalen eller gjeldende personopplysningslov, kan den Behandlingsansvarlige pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Brudd på denne avtalen er å regne som mislighold av Hovedavtalen.

Eventuelle endringer til denne avtalen skal beskrives i bilag 1 - Endringer.

# 12. Tilbakeføring ved opphør

Ved opphør av Hovedavtalen plikter databehandler å tilbakelevere alle Personopplysninger som er mottatt på vegne av Behandlingsansvarlig, og som omfattes av denne avtalen.

Ved opphør av avtalen skal Databehandler deretter endelig slette eller forsvarlig destruere alle dokumenter, data, disketter, lagringstape, cd-er, minnepinner/ «USB-sticks» og annet som inneholder Personopplysninger som omfattes av avtalen.

Dette gjelder også for eventuelle sikkerhetskopier. Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Databehandler skal uansatt lagre dokumentasjon på sikkerhetsrutiner i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave, og må i lagringstiden bistå Behandlingsansvarlig med å fremskaffe slik dokumentasjon.

# 13. Lovvalg og verneting

Avtalen følger lovvalgs- og vernetingsreglene i hovedavtalen.

## Bilag 1 Oversikt over godkjente underleverandører:

| Navn | Kontaktopplysninger | Behandles Personopplysninger innenfor/ utenfor EU |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Bilag 2 Endringer i databehandleravtalen

| Dato | Endringer gjelder punkt | Beskrivelse |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |